

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenji KOJIMA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: IC CARD, AND METHOD AND PROGRAM FOR PREVENTING ILLEGAL USE OF IC CARD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

Japan

APPLICATION NUMBER

2002-373565

MONTH/DAY/YEAR

December 25, 2002

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number

Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and


☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 2 5 日
Date of Application:

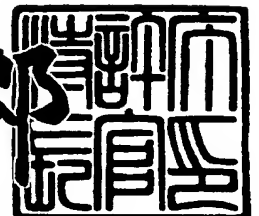
出 願 番 号 特 願 2 0 0 2 - 3 7 3 5 6 5
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 7 3 5 6 5]

出 願 人 株式会社東芝
Applicant(s):

2 0 0 3 年 7 月 8 日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



【書類名】 特許願

【整理番号】 13B02Y0401

【あて先】 特許庁長官殿

【国際特許分類】 G06K 19/00

【発明の名称】 I C カード、I C カードの不正利用防止方法、および、
プログラム

【請求項の数】 9

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

 【氏名】 小島 健司

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

 【氏名】 梅澤 健太郎

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

 【氏名】 三宅 秀享

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

 【氏名】 松下 達之

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

 【氏名】 友枝 裕樹

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 清水 秀夫

【発明者】

【住所又は居所】 神奈川県横浜市磯子区新杉田町 8 番地 株式会社東芝
横浜事業所内

【氏名】 渡辺 浩志

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100083161

【弁理士】

【氏名又は名称】 外川 英明

【電話番号】 (03)3457-2512

【手数料の表示】

【予納台帳番号】 010261

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ICカード、ICカードの不正利用防止方法、および、プログラム

【特許請求の範囲】

【請求項1】 利用時に外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うICカードにおいて、

このICカードに固有の認証情報を記憶する記憶手段と、

利用時に該端末より送信される認証情報を入力する入力手段と、

利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマと、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する判断手段と、

前記判断手段によって一致しないと判断された場合に、前記経時変化タイマへ計測の開始を指示するとともに、前記経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを、備えたことを特徴とするICカード。

【請求項2】 利用時に外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うICカードにおいて、

このICカードに固有の認証情報を記憶する記憶手段と、

利用時に該端末より送信される認証情報を入力する入力手段と、

利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する第一経時変化タイマと、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する第一判断手段と、

前記第一判断手段によって一致しないと判断される回数を、少なくとも予め定めた上限値までカウントするカウント手段と、

前記カウント手段でカウントされた回数が上限値になった場合に、前記第一経

時変化タイマへ計測の開始を指示するとともに、前記第一経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを備えたことを特徴とする IC カード。

【請求項 3】 利用時外のときにも電力供給を受けずに、前記第一経時変化タイマの経時変化部とは経時変化が異なる経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する第二経時変化タイマを更に備え、

前記制御手段は、前記第一判断手段で不正であると判断された都度、前記第二経時変化タイマへ計測の開始を指示するようにしたことを特徴とする請求項 2 記載の IC カード。

【請求項 4】 利用時外のときにも電力供給を受けずに、前記第一経時変化タイマの経時変化部とは経時変化が異なる経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する第二経時変化タイマを更に備え、

この第二経時変化タイマは、前記カウント手段でカウントが開始される時点から所定期間計測するものであることを特徴とする請求項 2 記載の IC カード。

【請求項 5】 前記第一経時変更タイマが未計測で、前記第二経時変化タイマが計測中で、前記第一判断手段で正当であると判断されたとき、前記第二経時変化タイマの計測を終了するようにしたことを特徴とする請求項 3 または 4 いずれかに記載の IC カード。

【請求項 6】 固有の認証情報を記憶する記憶手段と、利用時に外部の端末より送信される認証情報を入力する入力手段と、利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマとを備え、利用時に前記外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行う IC カードの不正利用防止方法であって、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断し、

この判断の結果、一致しないと判断された場合に、前記経時変化タイマへ計測

の開始を指示するとともに、前記経時変化タイマの計測中には、前記所定の処理を行わないようにしたことを特徴とする IC カードの不正利用防止方法。

【請求項 7】 固有の認証情報を記憶する記憶手段と、利用時に外部の端末より送信される認証情報を入力する入力手段と、利用時外の際にも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマとを備え、利用時に前記外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行う IC カードの不正利用防止方法であって、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合して、一致しない回数をカウントし、

このカウントした回数が予め定められ回数になった場合に、前記第一経時変化タイマへ計測の開始を指示するとともに、前記第一経時変化タイマの計測中には、前記所定の処理を行わないようにしたことを特徴とする IC カードの不正利用防止方法。

【請求項 8】 固有の認証情報を記憶する記憶手段と、利用時に外部の端末より送信される認証情報を入力する入力手段と、利用時外の際にも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマと、利用時に前記外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うプロセッサとを備える IC カードの前記プロセッサで実行されるプログラムであって、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する判断機能と、

前記判断機能での判断の結果、一致しないと判断された場合に、前記経時変化タイマへ計測の開始を指示するとともに、前記経時変化タイマの計測中には、前記所定の処理を行わないよう制御する制御機能とを備えたことを特徴とする IC カードの前記プロセッサで実行されるプログラム。

【請求項 9】 固有の認証情報を記憶する記憶手段と、利用時に外部の端末より送信される認証情報を入力する入力手段と、利用時外の際にも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化

の結果を示す信号を出力する経時変化タイマとを備え、利用時に前記外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うプロセッサとを備える IC カードの前記プロセッサで実行されるプログラムであって、

前記入力手段からの認証情報を、前記記憶手段の認証情報と照合して、一致しない回数をカウントするカウント機能と、

前記カウント機能でのカウントした回数が予め定められ回数になった場合に、前記第一経時変化タイマへ計測の開始を指示するとともに、前記第一経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御機能とを備えたことを特徴とする IC カードの前記プロセッサで実行されるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、接触型で、電池を備えない IC カードに係り、特に、所有者の誤入力による不備と他人のなりすましによる不正利用とを考慮した IC カード、IC カードの不正利用防止方法、および、プログラムに関する。

【0002】

【従来の技術】

IC カードは、個人情報をはじめとした重要情報を記録し利用するため、紛失時の正当な所有者以外の者による不正利用を防止する必要がある。このため、一般的な IC カードでは、IC カードを利用する際には、IC カードの正当な所有者（これを単に所有者と呼ぶ）を認証するために、PIN (Personal Information Number) による認証（これを PIN 認証と呼ぶ）が行われている。通常、正当な PIN の情報は IC カード内に記憶されており、所有者は IC カードを挿入した端末装置より PIN を入力し、その PIN が IC カード内で正当な PIN と照合された後、照合結果が端末装置に返される（例えば、特許文献 1 参照）。

【0003】

この PIN 認証では、他人の IC カードを手に入れた攻撃者が、所有者の PIN を推定し入力することで正当な所有者になりすます恐れがある。このような P

IN推定攻撃に対する対策としては、不正なPINが連続して一定回数入力された時点でICカードをロック（これをICカードのPINロックと呼ぶ）するという方法が行われている。PINロックされたICカードには、それ以上PINを入力することはできず使用不可能となる。なお、PINロックは、システム側で行う方式とICカード側で行う方式とがある。

【0004】

このようなPINロックは、不正な攻撃者に対しての対策であったが、所有者も誤って不正なPINの入力を行ってPINロックされてしまうことがある。この場合には、システムの管理者などに連絡し面倒な手続を行って、ロックを解除してもらう必要があり、所有者にとって使い勝手が悪かった。

【0005】

【特許文献1】 特開2000-76402公報

【0006】

【発明が解決しようとする課題】

ところで、従来技術で説明したICカードのPINロックは、ロックする時間を一定時間とすることができれば、正当なユーザには、特に管理者等へ連絡を行って面倒な手続を行うことなく、（しばらくは利用できないが）再び利用できるようになり、また、不正なユーザには、連続的に推定攻撃ができなくなるようになる。従って、ロックする時間を一定時間とすることが望まれていた。

【0007】

しかしながら、PINロックをシステム側で行う方式では、システム側の端末装置を集中管理するサーバ装置によってPINロックを管理するためのロック管理情報を集中管理しておき、PIN認証が行われる都度、管理されるロック管理情報をアクセスして判断する必要があり、処理が重くなる。

【0008】

そこで、PINロックをICカード側で行う方式で実現したいが、ICカード単体時には電力供給を得ることができないので、一定時間を計測することができなかった。なお、電池を内蔵することが考えられるが、これでは、電池が不要なICカードのメリットを生かせない。

【0009】

本発明は、上記問題点に鑑みなされたものであり、端末装置や処理サーバなどのシステム側に負担をかけず、電力供給の無い状態でも所定期間のPINロックを実現できるICカード、ICカードの不正利用防止方法、および、プログラムを提供することを目的とする。

【0010】

【課題を解決するための手段】

本発明は、利用時に外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うICカードにおいて、このICカードに固有の認証情報を記憶する記憶手段と、利用時に該端末より送信される認証情報を入力する入力手段と、利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する経時変化タイマと、前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する判断手段と、前記判断手段によって一致しないと判断された場合に、前記経時変化タイマへ計測の開始を指示するとともに、前記経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを備えた。

【0011】

また、本発明は、利用時に外部の端末と電氣的に接続し、電力供給を受けて所定の処理を行うICカードにおいて、このICカードに固有の認証情報を記憶する記憶手段と、利用時に該端末より送信される認証情報を入力する入力手段と、利用時外のときにも電力供給を受けずに経時変化する経時変化部を有し、該電力供給中に所定の指示により経時変化の結果を示す信号を出力する第一経時変化タイマと、前記入力手段からの認証情報を、前記記憶手段の認証情報と照合し、一致するか一致しないかを判断する第一判断手段と、前記第一判断手段によって一致しないと判断される回数を、少なくとも予め定めた上限値までカウントするカウント手段と、前記カウント手段でカウントされた回数が上限値になった場合に、前記第一経時変化タイマへ計測の開始を指示するとともに、前記第一経時変化タイマの計測中には、前記所定の処理を行わないように制御する制御手段とを備

えた。

【0012】

このようにした本発明のICカードは、ICカード側で、一定時間のPINロックを可能にすることができ、ICカードへのPINの推定攻撃に対する安全性を確保しつつ、利用者の利便性も確保できる。

【0013】

【発明の実施の形態】

以下、本発明の実施形態について、図面を参照しつつ詳細に説明する。

【0014】

図1は、本実施の形態に係る全体システムを示したものであり、ICカード端末10と、接触型のICカード20とからなる。なお、ICカード端末10は、ネットワークを介して、多数のICカード端末10を集中管理するサーバ等と接続されていて良いことは、勿論である。

【0015】

接触型のICカード20は、プラスチックでカード状の定格サイズで形成されたプラスチック部材25と、所定の論理動作を行うICチップ22を封止材23で封止し、このICチップ22と接続され、外部に露出するICカードインタフェース21を備えるICモジュール24とを備え、ICカード端末10へ挿入中に、ICカード端末10からの電源供給を受けて、ICチップ22が動作し、一方、ICカード端末10へ挿入されない時は動作しないものである。

【0016】

ICカード端末10は、ICカード20を挿入するための挿入部11と、挿入部11にICカード20が挿入された際に、ICカード20と電氣的に接続するICカードインタフェース13とを備える。ICカードインタフェース13は、ICカード20が挿入された際に、ICカード20のICカードインタフェース21と対向する位置に配置される。また、ICカード端末10は、ICカード20の挿入後、ユーザからのPIN (Personal ID Number) を入力するための入力部12と、ICカード端末10の全体の制御を司る制御部14とを備える。入力部12、制御部14、及びICカード20への電力を供給する

ための電源Vは、ICカードインタフェース13と接続されている。

【0017】

このように構成される本システムにおいてICカード20を利用する際には、まずICカード20をICカード端末10へ挿入し、入力部12からPINを入力し、この入力されたPINをICカードインタフェース13、21を介し、ICカード20のICチップ22へ供給する。ICチップ22では、供給されたPINを、ICチップ22の内部で記憶する正当なPINと照合する。この照合結果が正しければ、その後、ICカード端末10からICカード20へICカードインタフェース13、21を介し、コマンドを送信し、ICカード20は、この命令を解釈し動作する。また、ICカード20は、ICカード端末10へ応答、等を行う。

【0018】

図2は、ICカード20のICチップ22の内部構成を示している。

【0019】

入出力部31は、ICカードインタフェース21と内部バス39とに接続され、このICカード20がICカード端末10へ挿入中に、ICカードインタフェース21を介して得られた電力を電源供給部38へ供給するとともに、ICカードインタフェース21を介して受信したコマンドやデータを内部バス39へ送信するとともに、内部バス39から受信されるコマンドやデータをICカードインタフェース21へ送信する。

【0020】

CPU32は、ICチップ22の全体を制御するものであり、ROM33に記憶されるプログラムによって、動作する。ROM33には、プログラムの他にこのICカード20のPINが記憶されている。このROM33に記憶されるPINの値を、以後、正当なPIN、それ以外のPINの値を不正なPINと呼ぶことにする。なお、PINの変更を許容するICカード20を提供する場合には、後記のEEPROM35に記憶するようにしても良い。また、ROM33には、更に所定期間中に不正なPINが入力される回数を制限するための閾値が記憶されている。

【0021】

RAM34は、CPU32に利用されるワークメモリである。EEPROM35は、CPU32によって読み書き可能な不揮発性の半導体メモリである。EEPROM35には、所定期間中に入力される不正なPINの回数を記憶するための不正カウント数記憶領域を備えている。

【0022】

電源供給部38は、入出力部31と接続され、ICカード端末10から供給される電力を受け、ICチップ22内の各部に電源供給を行うものである。

【0023】

ロック用タイマ36、及びカウンタ用タイマ37は、同様な構成で実現され、電源供給を受けることなく経時変化することにより所定期間が経過したか否かを測定するものである。なお、ロック用タイマ36、及びカウンタ用タイマ37は、測定する所定期間はそれぞれ固定であり、それぞれ期間が異なっており、ロック用タイマ36のほうが長い期間カウントできる。ロック用タイマ36は、後記のICカード20内で行われる他の処理が行えない（ロック状態）期間を設定するものである。一方、カウンタ用タイマ37は、不正なPINをカウントするための期間を設定するものである。

【0024】

ここで、このロック用タイマ36及びカウンタ用タイマ37（以下総称して単にタイマ36／37と称す）についてより詳細に説明する。

【0025】

図3は、タイマ36／37の基本概念を示したものである。タイマ36／37は、電池などの電力源無く経時変化する経時変化部41と、この経時変化部41へ入力信号を入力する入力部42と、経時変化部41の状態に基づいて、入力信号に対し変化した出力信号を出力する出力部43とを備える。ここで、経時変化部41は、時間とともに状態が変化するものであり、この変化した状態を時間の測定に利用するものである。入力部42及び出力部43は、経時変化部41の状態を確認したいときに用いられる。

【0026】

図4は、図3のタイマ36／37の基本概念を実現する第一の具体例である。

【0027】

この第一の具体例のタイマは、ソース領域51と、ドレイン領域52と、ソース領域51およびドレイン領域52との間にチャネル領域53とからなる第1層と、第1層の上部に積層されるトンネル絶縁膜54からなる第2層と、第2層の上部に積層されるフローティングゲート55からなる第3層と、第3層の上部に積層される絶縁膜56で形成される第4層と、第4層の上部に積層される制御ゲート57からなる第5層とを備えて形成される。また、ソース領域51、及び、ドレイン領域52には、それぞれソース電極58とドレイン電極59とが設けられている。

【0028】

図5は、図4のタイマ36／37が時間経過に伴った状態変化を示した図である。なお、図上、グレーの丸は電子を示しており、白の丸は正孔を示している。

【0029】

(a)は、初期状態を示す図である。タイマ36／37は、前処理として、制御ゲート57からチャネル領域53の基板界面とフローティングゲート55の間に高電界を印加し、FNトンネリングによって電子をチャネルからフローティングゲート55に注入しておく。このとき、チャネル領域53の基板界面は、反転して正孔が集中し、ソース領域51とドレイン領域52との間のチャネル領域53の基板界面にチャネルが開く。

【0030】

この(a)の状態から、時間経過と共に、フローティングゲート55の電子が基板界面に直接トンネルし、徐々にチャネル領域53の基板界面の電界が減少する。(b)は、(a)の状態からある時間だけ経過した後の時刻 T_1 の状態を示しており、(c)は、(b)の状態から更にある時間だけ経過した後の時刻 T_2 の状態を示しており、(d)は、(c)の状態から更にある時間だけ経過した後の時刻 T_3 の状態を示している。なお、点線は、電子がその時刻までに直接トンネルにより移動したことを模式的に示している。時刻 T_3 の(d)の状態では、フローティングゲート55に注入されていた電子がほとんど抜け、チャネル領域

53の基板界面にチャンネルが形成されなくなり、その結果、出力信号が流れなくなる。

【0031】

図6は、このようなタイマ36/37の時間と出力信号との関係を示した図である。時刻 $T_a (=0)$ から T_b の間に直接トンネリングが生じ、最後にはチャンネルが消失してノイズレベルまで出力信号が低下する。タイマ36/37は、時刻 $T_a (=0)$ から $T_b (=ノイズレベル到達時間)$ の間の、この経時変化を利用し変化した出力信号を供給するから、この出力信号を受信する側は、例えば、所定期間経過したか否か判断したり、このタイマ36/37の状態と出力信号の関係が逐時明確になっている場合には、初期状態からの相対的な時刻を知ることができる。なお、図6上の T_1 、 T_2 、 T_3 は、図6の(b)、(c)、(d)の状態を示している。

【0032】

図7は、図3のタイマ36/37の基本概念を実現する第二の具体例である。この第二の具体例のタイマ36/37は、ソース領域61と、ドレイン領域62と、ソース領域61およびドレイン領域62との間にチャンネル領域63とからなる第1層と、第1層の上部に積層されるトンネル絶縁膜64からなる第2層と、第2層の上部に積層されるゲート65からなる第3層と、第3層の上部にリーク電流を制御するためのPN接合66とを備えて形成される。また、ソース領域61、及び、ドレイン領域62には、それぞれソース電極68とドレイン電極69とが設けられている。

【0033】

タイマ36/37の時間経過に伴った状態変化についての説明は、第一の具体例のタイマ36/37の説明での直接トンネリングを、PN接合のリーク電流に置き換えれば第一の具体例と同様なので省略する。

【0034】

図8は、図3のタイマ36/37の基本概念を実現する第三の具体例である。この第三の具体例のタイマ36/37は、ソース領域71と、ドレイン領域72と、ソース領域71およびドレイン領域72との間にチャンネル領域73とからなる

る第1層と、第1層の上部に積層されるトンネル絶縁膜74からなる第2層と、第2層の上部に積層されるゲート75からなる第3層と、第3層の上部にリーク電流を制御するためのショットキー接合76とを備えて形成される。また、ソース領域71、及び、ドレイン領域72には、それぞれソース電極78とドレイン電極79とが設けられている。

【0035】

タイマ36/37の時間経過に伴った状態変化についての説明は、第一の具体例のタイマ36/37の説明での直接トンネリングを、PN接合のリーク電流に置き換えれば第一の具体例と同様なので省略する。

【0036】

以上説明したタイマ36/37は、図9に示す接続例のようにして構成し、利用する。

【0037】

図9(a)の例は、タイマ36/37の両端に、電源供給部38から電源供給される時に電圧をかけることが可能なようになっており、電源端81側には、スイッチ素子83を介してタイマ36/37のソース電極58/68/78が接続され、GND端82側とは電流計84を介し、ドレイン電極59/69/79が接続される。スイッチ素子83は、CPU32からのON/OFF（イネーブル）信号線と接続され、ON信号時にスイッチがONされ導通する。また、電流計84は、CPU32へ電流値を出力するよう接続される。

【0038】

そして、ICチップ22が動作中にタイマ36/37の状態を確認する際には、CPU32がスイッチ素子83をONにすると、電源端81-GND端82間に所定電圧がかかり、タイマ36/37を介して流れる電流を電流計84で測定し、測定された電流値がCPU32へ出力されることによって、CPU32は、タイマ36/37の状態が分かるようになる。

【0039】

また、特に図示しないが、タイマ36/37は、図5の説明時に記載したように時間を測定する前に、前処理が必要であり、この前処理を行う手段を備えてい

る。タイマ36／37は、外部から計測開始の指示を受けると、前処理を行った上で、時間計測を開始する。

【0040】

上記接続例では、一つのタイマ36／37についての例を示したが、複数のタイマ37を備えるようにしてもよい。複数のタイマ36／37の各経時変化部41の経時変化は、用途に応じて同じであっても、異なっても良いが、ここでは同じ例を図9（b）に示し説明する。この例は、（a）のタイマ36／37を複数並列化し、それぞれ出力される電流値を平均化回路85へ入力し、平均化した電流値を制御回路34へ出力するようにしたものである。なお、制御回路34からのON／OFF（イネーブル）信号線もそれぞれのスイッチ素子83へ接続されて、共通に制御できる。この例では、経時変化部41の経時変化に多少のばらつきがあっても、平均化することにより、安定したタイマを提供できる。また、特に図示しないが、複数の経時変化部41の経時変化が異なったものとする、いろいろな時刻情報が取得できるなどの利点がある。

【0041】

次に、本チップ22のCPU32上で動作する全体の概略フローについて、図10を用いて説明する。

【0042】

ICカード20がICカード端末10へ挿入されてから排出までに、まず、必ずPIN認証を行い、このPIN認証の結果が正当なPINと判断されたときに、他の処理が行えるようになっている。PIN認証の結果が不正なPINと判断されたときには、カードを一旦排出するようにする（図の（a））、または、カードを排出せずに再度PIN認証を行わせるようにする（図の（b））。

【0043】

次に、このPIN認証に関する動作について、図11のフローチャートを用いて詳細に説明する。

【0044】

まず、ユーザは、ICカード20をICカード端末10へ挿入の上、入力部12から、PINを入力する。入力されたPINは、ICカードインタフェース1

3、21を介して、ICカード20の入出力部31へ入力される。入出力部31は、CPU32へPINを送信し、CPU32で動作するプログラムは、PINを受信する(S101)。

【0045】

PINを受信すると、まず、ロック用タイマ36が現在計測中であるか否かを判断する(S102)。これは、ロック用タイマ36から図9の説明時に説明したようにして電流値を読み取り、この電流値が、ノイズレベルに到達しているか否かを判断すればよい。

【0046】

もし、計測中であると判断された場合には、ICカード20は、現在ロック状態であるため、失敗と判断し、端末10へその旨通知する(S103)。

【0047】

一方、ロック用タイマ36が計測中で無いと判断された場合、次にカウンタ用タイマ37が計測中であるか否かを判断する(S104)。これも、ステップS102と同様の方法で判断すれば良い。

【0048】

もし、カウンタ用タイマ37が計測中で無ければ、EEPROM35の不正カウンタ数記憶領域に記憶される不正カウンタをリセットし(S105)、カウンタ用タイマ37の計測を開始させる(S106)。この開始の指示によりカウンタ用タイマ37は、例えば、上記で説明した第一の具体例のタイマであったとすると、一瞬の間高電圧を印加することにより、フローティングゲートへ電子を蓄え、その後何もしないことにより計測を開始する。

【0049】

次に、ステップS101で受信したPINを、ROM33に記憶する正当なPINと照合する(S107)。

【0050】

この照合の結果、受信したPINが正しいPINであれば、カウンタ用タイマ37の計測を終了し(S108)、成功と判断し、端末10へその旨通知する(S109)。なお、ステップS108の終了の処理は、カウンタ用タイマ37自身の経時変化

を終了させたり、カウンタ用タイマ37の有効／無効フラグを格納する領域をEEPROM35内に設けておき、これによって管理するようなど様々な方法で実現できる。

【0051】

一方、PIN照合の結果、不正なPINであれば、EEPROM35の不正カウンタ記憶領域に記憶する不正カウンタの値をインクリメントする(S110)。次に、このインクリメントした不正カウンタの値が、ROM33に格納される閾値か否かを確認する(S111)。

【0052】

不正カウンタ数格納領域の値が閾値となった場合には、ICカード20を正規のユーザでないユーザが不正利用している可能性が高いとして、ロック用タイマ36へ計測を開始させる(S112)。そして、ICカード20をロック状態に移行させる。なお、この計測の開始も、ステップS106の説明時に記載した方法と同様の方法で行えば良い。そして、ステップS107でのPIN照合の結果に基づき、失敗と判断し、端末10へその旨通知する(S113)。

【0053】

以上のようなPIN認証に関する動作についてのフローに従う一具体例のタイムチャートは、図12に示すようになる。なお、PINの不正入力の際の閾値を3とし、カウンタ用タイマ37が計測する時間をT1、ロック用タイマ36が計測する時間をT2とし、 $T1 < T2$ とする。また、不正PINは、入力部12から不正なPINが入力されたことを示し、正当PINは、入力部12から正当なPINが入力されたことを示している。

【0054】

図12(a)において、初期状態は不正カウンタは不定(何でも良い)、タイマ36、37は何れも計測していない状態である。この状態から、まず、最初の不正PINが入力されると、ステップS105によって不正カウンタをリセット(0)にし、ステップS106によってカウンタ用タイマ37が計測を開始し、ステップS110によって不正カウンタがインクリメントされ1となる。なお、この状態では、まだ閾値より不正カウンタのほう小さいのでステップS112は、未だ開始され

ない。

【0055】

次に、最初の不正PINが入力されてからT1までの期間より前に、再度、不正PINが入力されたとする。このとき、カウンタ用タイマ37は計測中であるから、ステップS105、S106の処理はされず、ステップS110によって不正カウンタがインクリメントされ2となる。なお、なお、この状態でも、まだ閾値より不正カウンタのほう小さいのでステップS112は、未だ開始されない。

【0056】

次に、最初の不正PINが入力されてからT1までの期間より前に、再度、不正PINが入力されたとする。このとき、カウンタ用タイマ37は計測中であるから、ステップS105、S106の処理はされず、ステップS110によって不正カウンタがインクリメントされ3となる。この結果、不正カウンタは閾値と同じになったので、ステップS112が実行される。すなわち、ロック用タイマ36が計測を開始し、ICカード20はロック状態となり、以後T2期間経過するまで継続する。このT2期間中は、例えば正当なPINが入力されたとしても、ステップS103で認証処理が終了するようになっており、ロック状態を維持している。

【0057】

T2時間経過するとロック用タイマ36は計測を終了するが、この時より前にカウンタ用タイマ37も（ $T1 < T2$ なので）計測を終了しており、上記で述べた初期状態と同様な状態に戻る。なお、不正カウンタの値は、次回のPIN入力時にステップS105によって必ずリセットされるので、初期状態のときと同様、不定と考えて良い。

【0058】

一方、図12（b）は、カウンタ用タイマ37でカウント中に正当なPINが受信された場合を示した図である。図12（b）において、初期状態、最初の不正PIN、2回目の不正PINは、図12（a）と同様とする。ここで、3回目のPINの受信時に、正当なPINが入力されると、ステップS101、S102、S104、S107の順に進み、ステップS107で正しいPINであると判断され、ステップS108へ進む、ステップS108では、カウンタ用タイマの計測を終了するので、初期状

態と同じ状態に戻ることになる。

【0059】

以上説明したように、本実施の形態の IC カードは、電力が供給されない状況でも動作し続けるタイマをロック用タイマとして利用するから、ロック状態後、一定時間後に再び PIN 受信可能状態となる。

【0060】

また、電力が供給されない状況でも動作し続けるタイマをカウンタ用タイマとして利用するから、最初の不正 PIN の入力後一定時間経過内にロック状態とならなければ、不正カウンタをリセットすることが可能となる。

【0061】

このようにすることは、正当なユーザが誤って不正 PIN を閾値数以上入力したとしても、一定時間経過するだけで、特に管理者側から何もすることなく再度利用可能になるだけでなく、不正なユーザが不正 PIN を多数入力することによって、正当な PIN を知りえる PIN の推定攻撃に対しても、一定時間経過するまで再度 PIN 入力ができなくなるので、正当な PIN を知るまでに大変時間がかかるようにできる。

【0062】

また、この IC カードを利用可能な端末は、従来の IC カード端末と何ら変更無く利用できる利点もある。

【0063】

次に、上記で説明した PIN 認証の別の変形例に関する動作について、図 13 のフローチャートを用いて詳細に説明する。

【0064】

変形例の PIN 認証のフローチャートは、図 11 の PIN 認証のフローチャート上のステップ S106 の「カウンタ用タイマ計測開始」の位置を、ステップ S107 の後に移動したものであり、他は特に変更点が無い。このような PIN 認証の別の変形例によれば、PIN 照合により、不正 PIN と判断された時に、カウンタ用タイマ 37 の計測をはじめから再度開始する。

【0065】

このようなPIN認証の別の変形例に従う、一具体例のタイムチャートは、図14のようになる。なお、図14の諸条件は、図12のそれと同様にしてある。

【0066】

図14(a)および(b)からわかるように、ロック用タイマ36が計測中で無い状態(不正カウンタが閾値を越えていない場合)では、カウント用タイマ37の計測時間は、計測開始後、不正PINが入力される都度、計測を再度開始し、結果として延長されている。また、図14(b)左のように、ロック用タイマ36が計測中で無い状態(不正カウンタが閾値を越えていない場合)で、且つ、カウント用タイマ37の計測中に、正当なPINが入力されると、カウント用タイマ37の計測を終了するようになる。一方、図14(b)右のように、ロック用タイマ36が計測中の状態(不正カウンタが閾値を越えている場合)では、不正PIN、正当PINの何れが入力されても、カウント用タイマ37には、何ら影響を受けない(延長されない)。

【0067】

以上のような変形例によれば、ロック状態になっていない状態では、最後にPIN入力を間違ってから所定時間中何もPIN入力しなければ、所定時間経過後には再度PIN入力ができるようになることを保証できる利点を(図11のフローと比較し)更に備えている。

【0068】

以上説明したように、本実施の形態のICカードの変形例は、電力が供給されない状況でも動作し続けるタイマをロック用タイマとして利用するから、ロック状態後、一定時間後に再びPIN受信可能状態となる。

【0069】

また、電力が供給されない状況でも動作し続けるタイマをカウンタ用タイマとして利用するから、前回の不正PIN入力後、一定時間経過していれば、不正カウンタをリセットすることが可能となる。

【0070】

このようにすることは、正当なユーザが誤って不正PINを閾値数以上入力したとしても、一定時間経過するだけで、特に管理者側から何もすることなく再度

利用可能になるだけでなく、不正なユーザが不正 P I N を多数入力することによって、正当な P I N を知りえる P I N の推定攻撃に対しても、一定時間経過するまで再度 P I N 入力ができなくなるので、正当な P I N を知るまでに大変時間がかかるようにできる。

【0071】

また、この I C カードを利用可能な端末は、従来の I C カード端末と何ら変更無く利用できる利点もある。

【0072】

【発明の効果】

以上説明したように、本発明によれば、I C カード側で、一定時間の P I N ロックを可能にすることができる。これにより、I C カードへの P I N の推定攻撃に対する安全性を確保しつつ、利用者の利便性も確保できる。

【図面の簡単な説明】

【図1】 本実施の形態に係る全体システムを示した図。

【図2】 I C カード 20 の I C チップ 22 の内部構成を示す図。

【図3】 タイマ 36 / 37 の基本概念を示した図。

【図4】 タイマ 36 / 37 を実現する第一の具体例。

【図5】 タイマ 36 / 37 が時間経過に伴った状態変化を示した図。

【図6】 タイマ 36 / 37 の時間と出力信号との関係を示した図。

【図7】 タイマ 36 / 37 の基本概念を実現する第二の具体例。

【図8】 タイマ 36 / 37 の基本概念を実現する第三の具体例。

【図9】 タイマ 36 / 37 と C P U 32 との接続例。

【図10】 本チップ 22 の C P U 32 上で動作する全体の概略フローチャート。

【図11】 P I N 認証に関する動作についてのフローチャート。

【図12】 P I N 認証に関する動作についてのフローに従う具体例のタイムチャート。

【図13】 P I N 認証に関する動作についての別の変形例のフローチャート。

【図14】 P I N 認証に関する動作についてのフローに従う具体例のタイムチャート。

ャート。

【符号の説明】

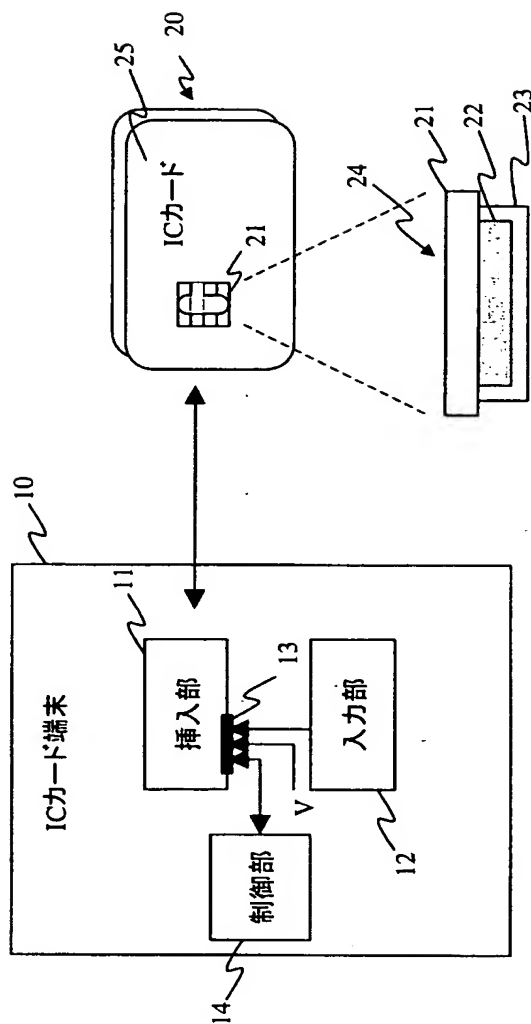
- 10…ICカード端末
- 11…挿入部
- 12…入力部
- 13…ICカードインタフェース
- 14…制御部
- 20…ICカード
- 21…ICカードインタフェース
- 22…ICチップ
- 23…封止材
- 24…ICモジュール
- 25…プラスチック部材
- 31…入出力部
- 32…CPU
- 33…ROM
- 34…RAM
- 35…EEPROM
- 36…ロック用タイマ
- 37…カウンタ用タイマ
- 38…電源供給部
- 39…内部バス
- 41…経時変化部
- 42…入力部
- 43…出力部
- 51、61、71…ソース領域
- 52、62、72…ドレイン領域
- 53、63、73…チャネル領域
- 54、64、74…トンネル絶縁膜

- 5 5 … フローティングゲート
- 5 6 … 絶縁膜
- 5 7 … 制御ゲート
- 5 8、6 8、7 8 … ソース電極
- 5 9、6 9、7 9 … ドレイン電極
- 6 5、7 5 … ゲート
- 6 6 … P N 接合
- 7 6 … ショットキー接合
- 8 1 … 電源端
- 8 2 … G N D 端
- 8 3 … スイッチ素子
- 8 4 … 電流計
- 8 5 … 平均化回路

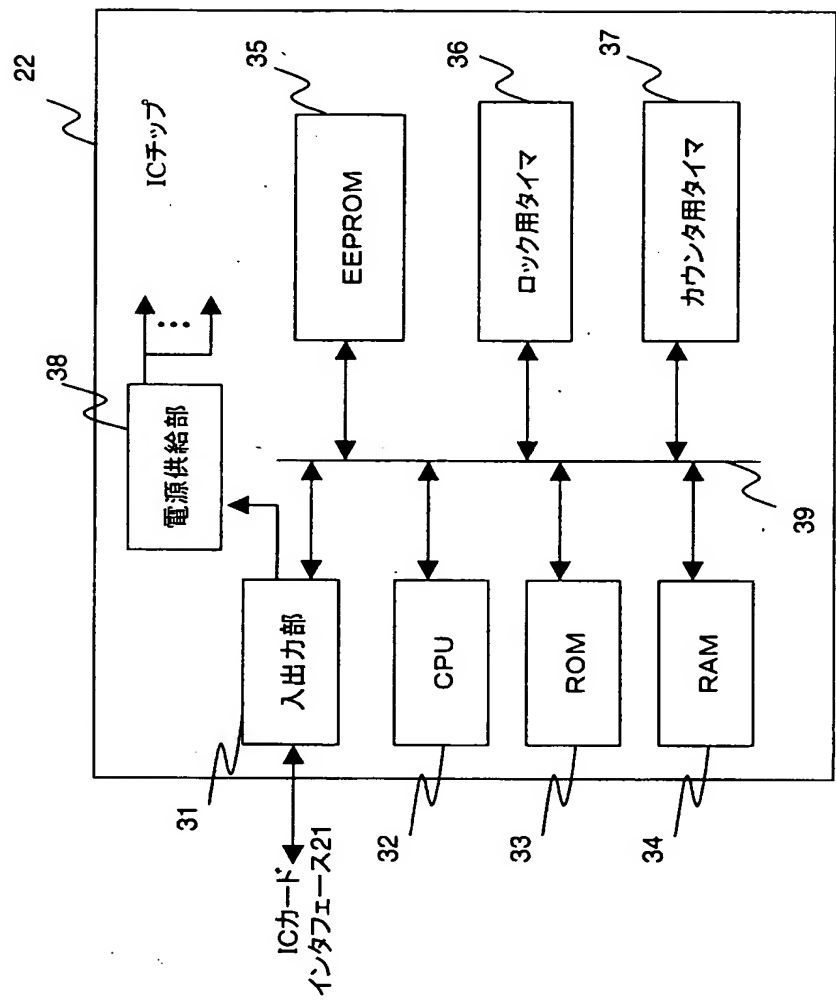
【書類名】

図面

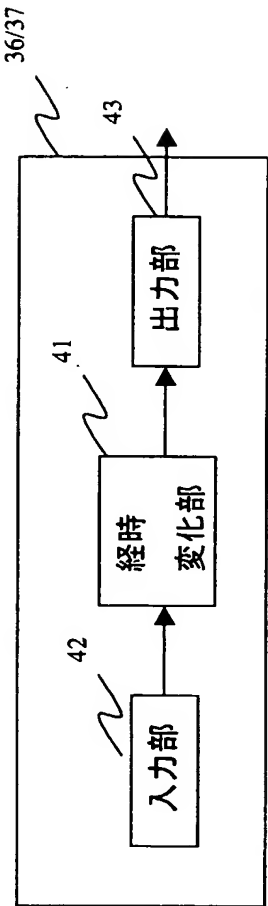
【図 1】



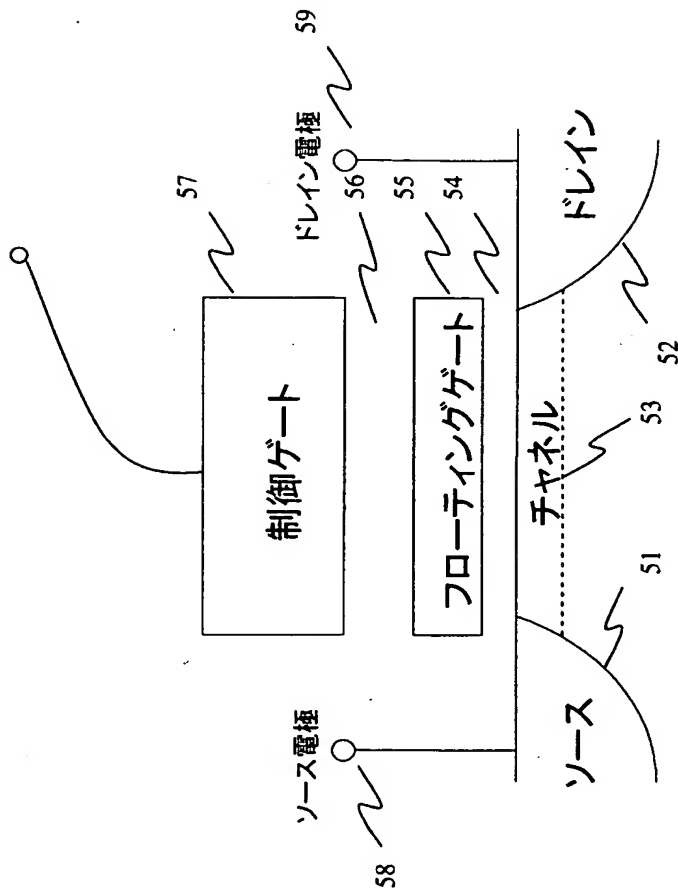
【図 2】



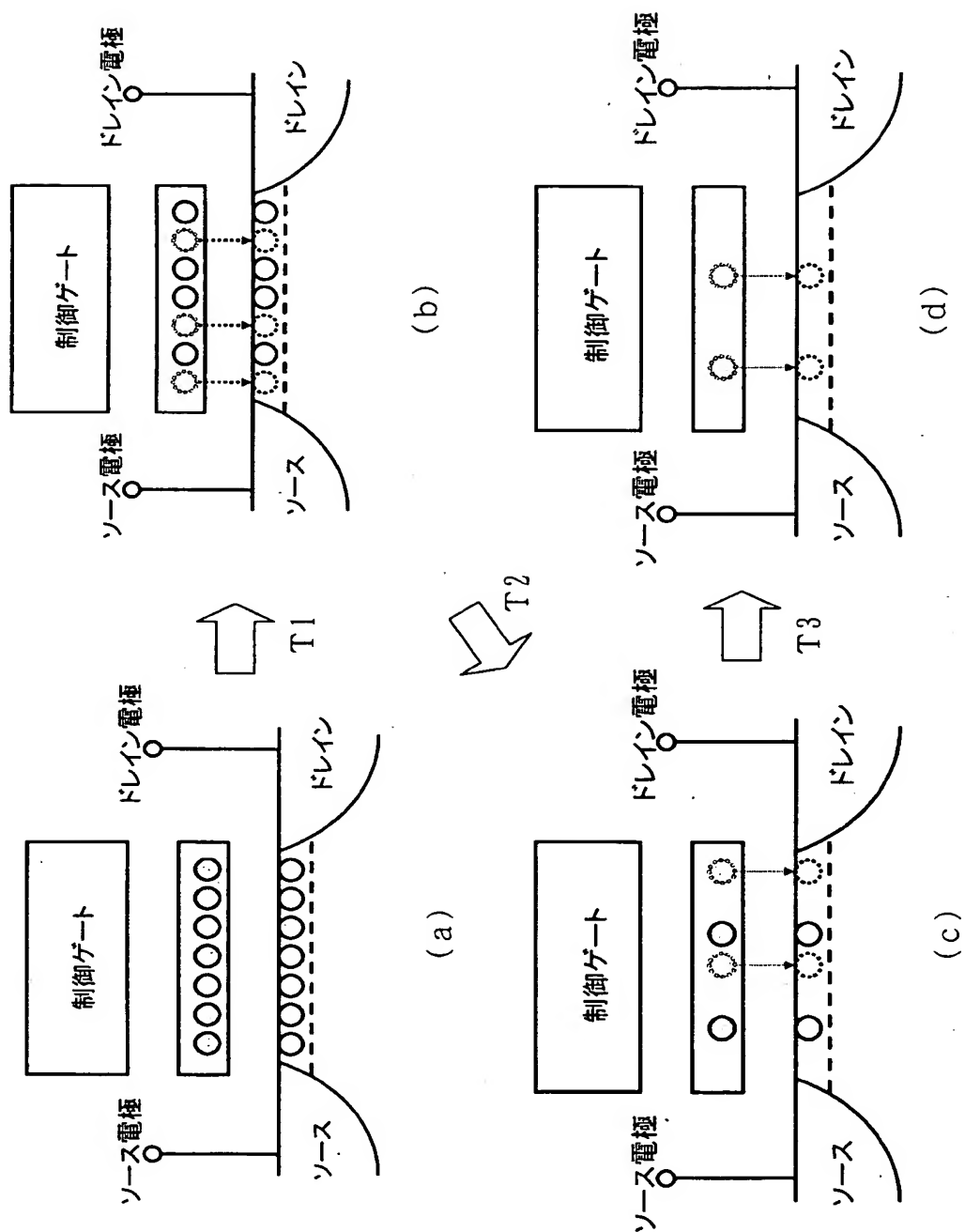
【図 3】



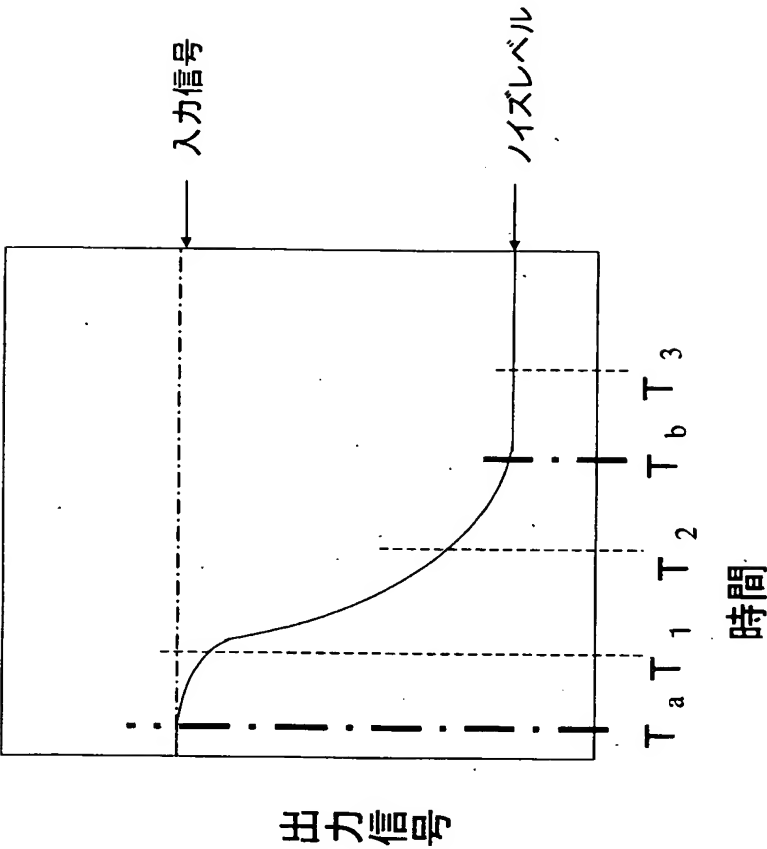
【図 4】



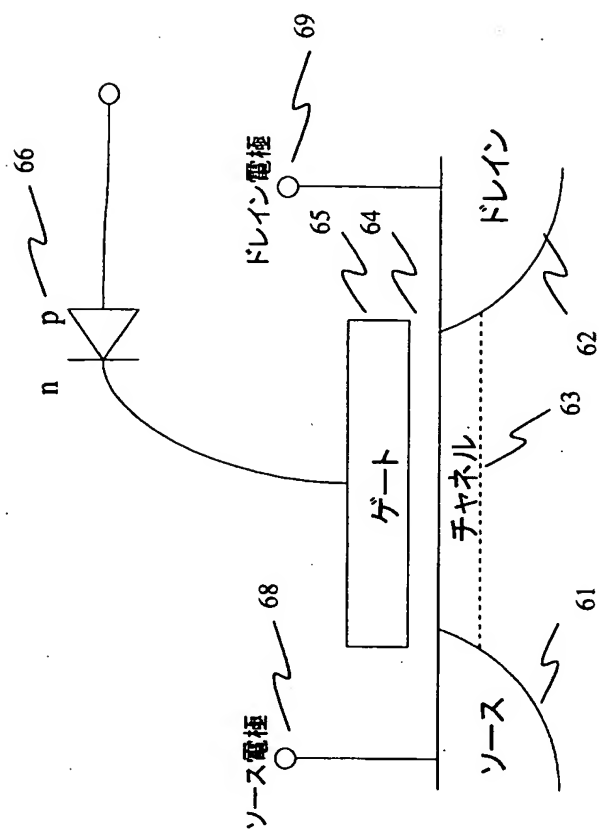
【図 5】



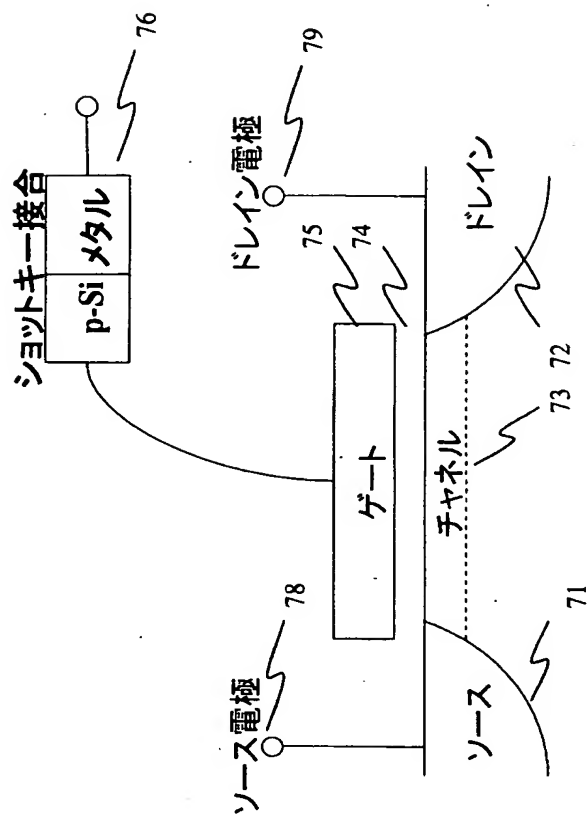
【図 6】



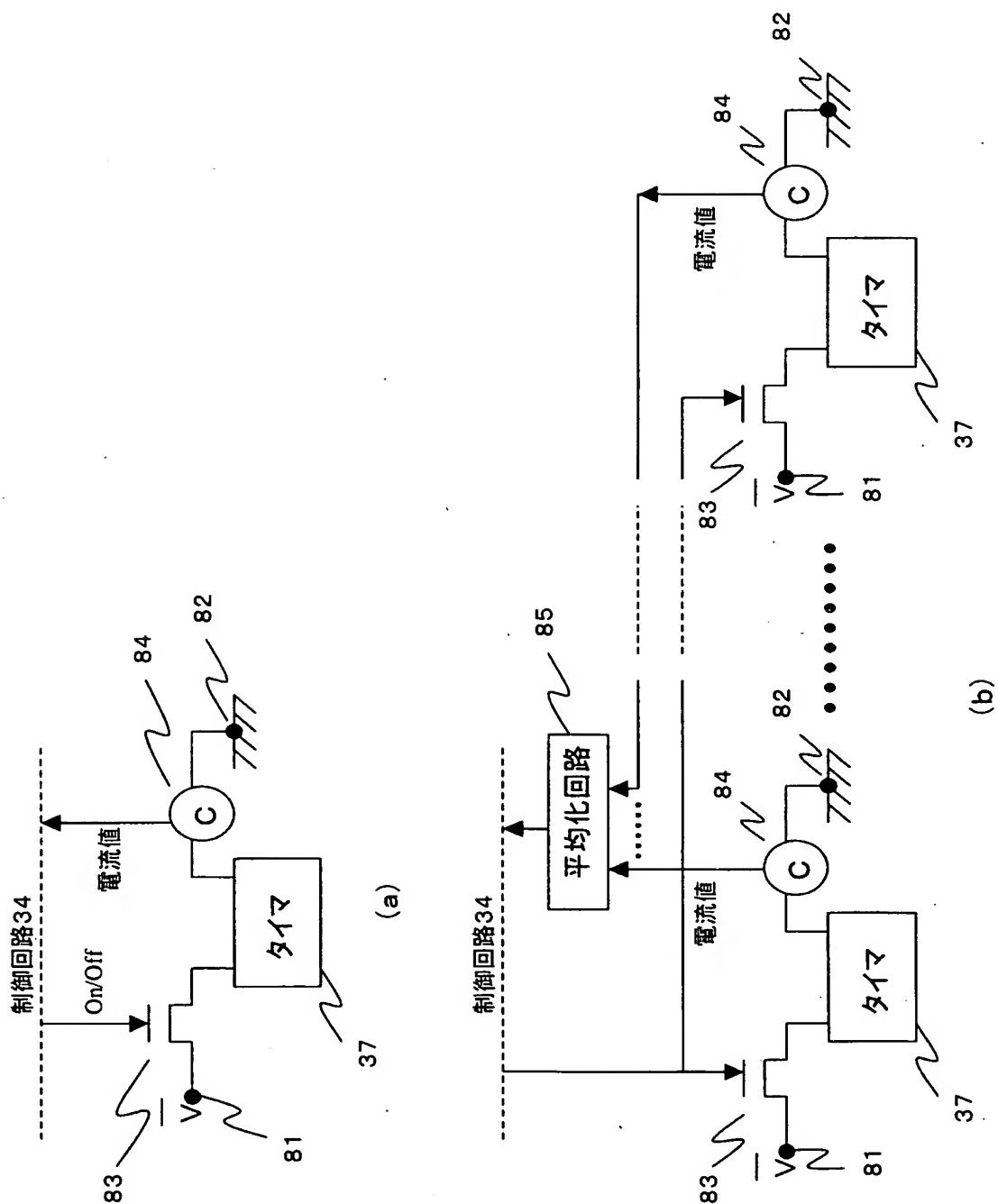
【図 7】



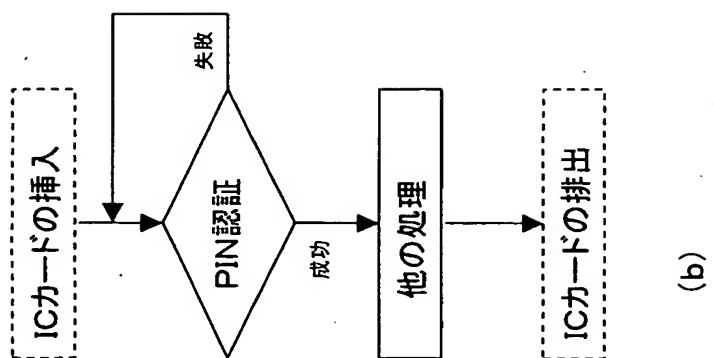
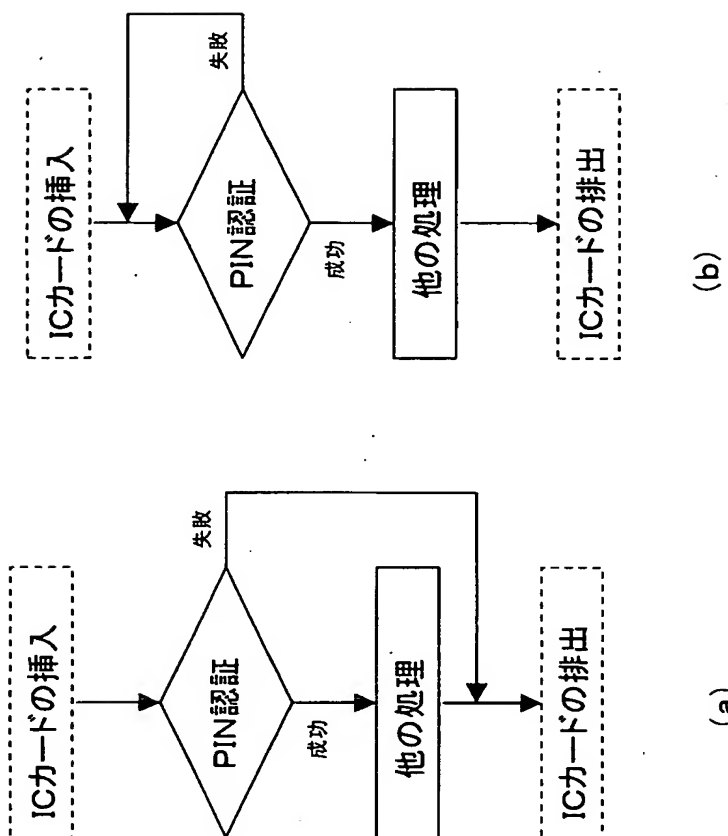
【図 8】



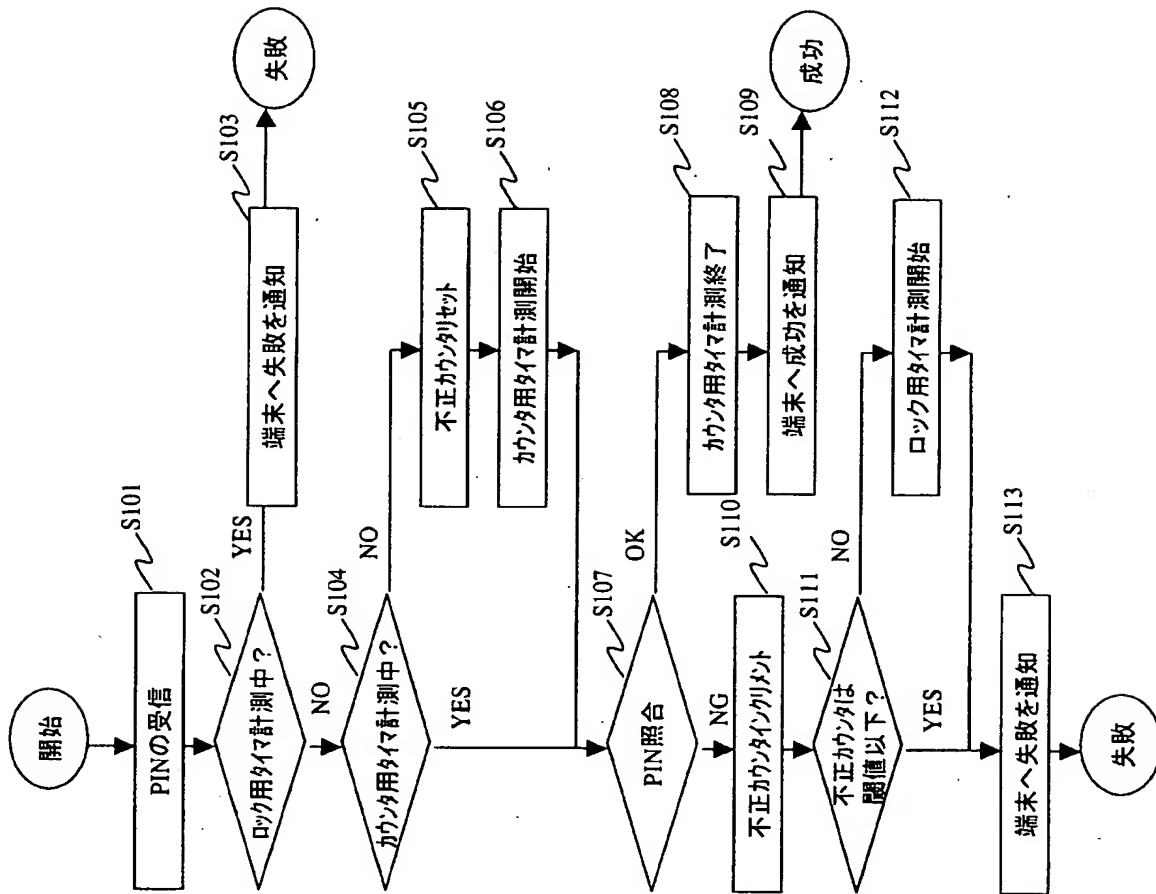
【図 9】



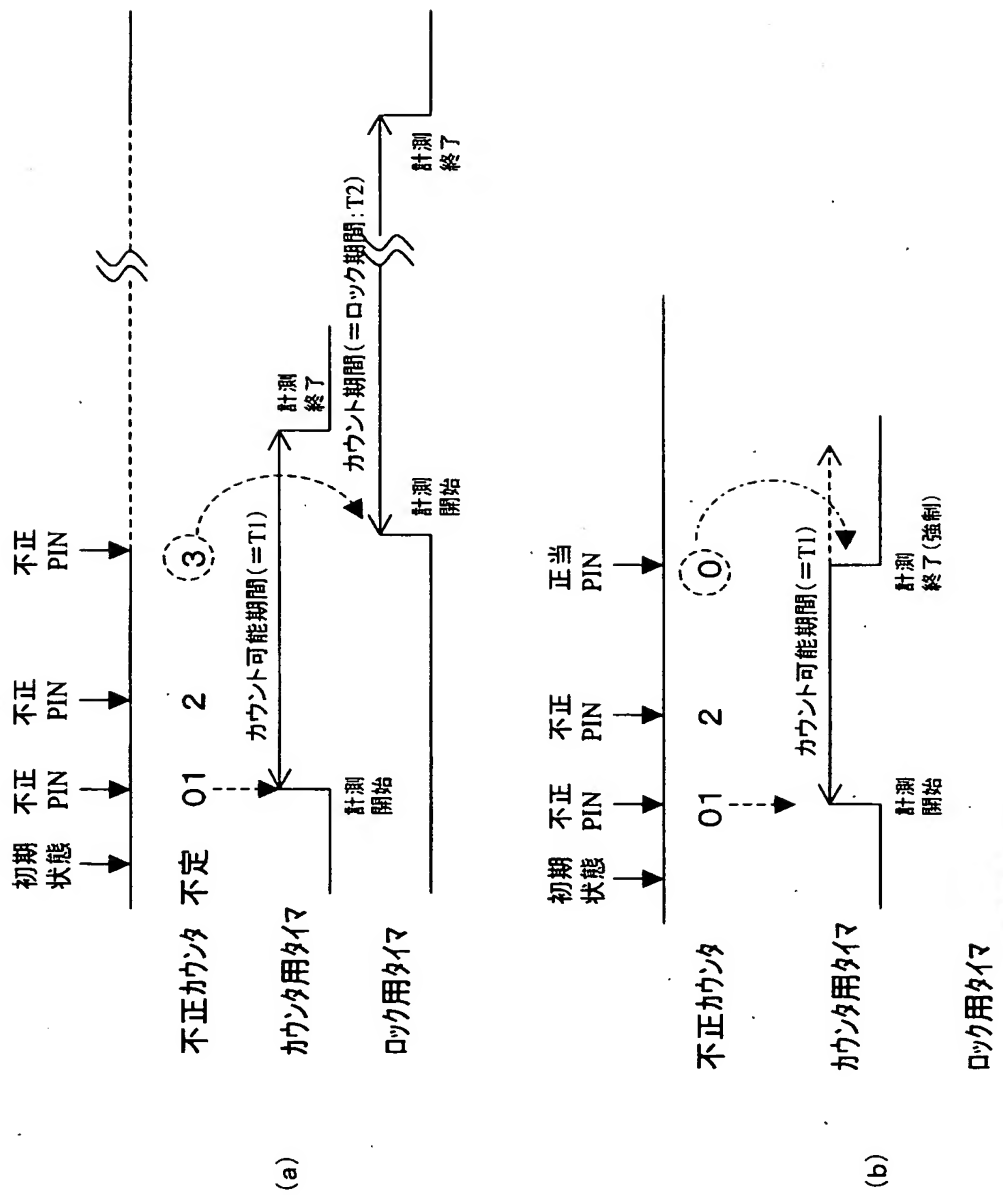
【図 10】



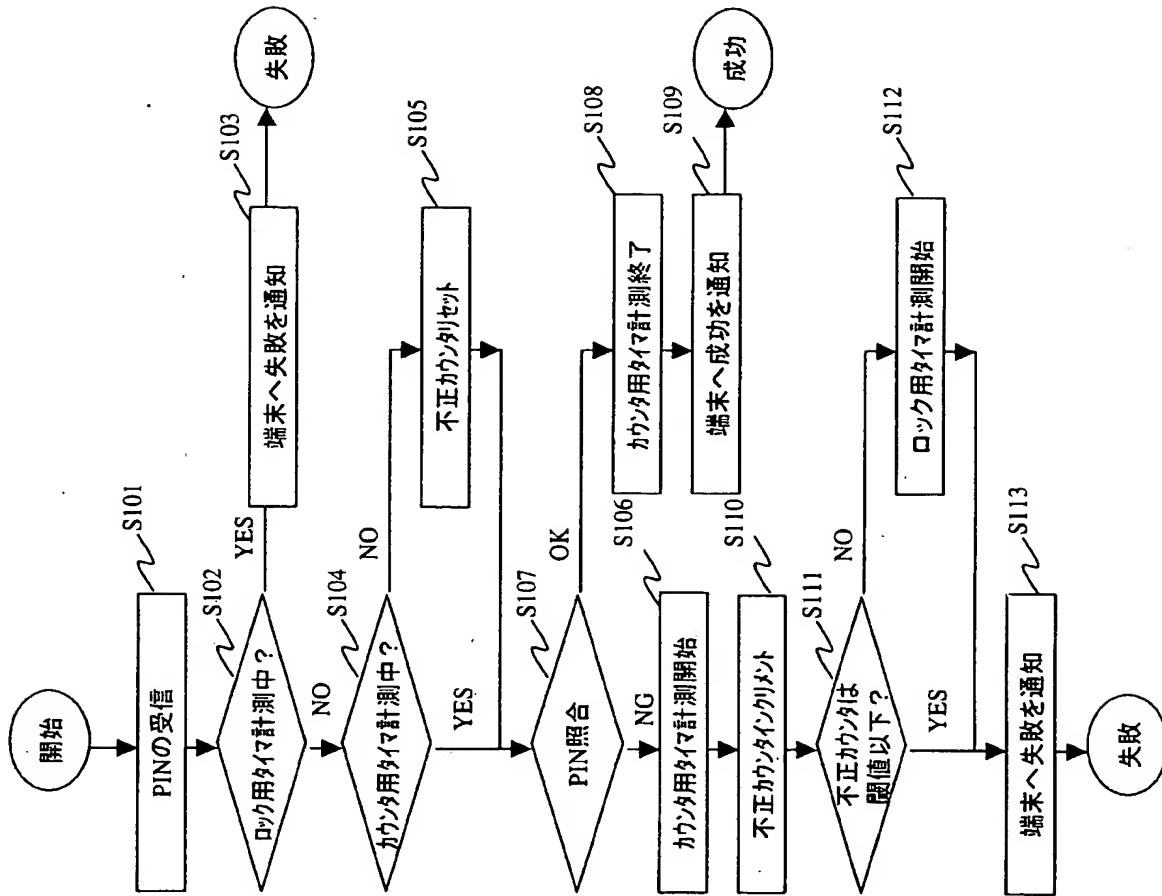
【図 11】



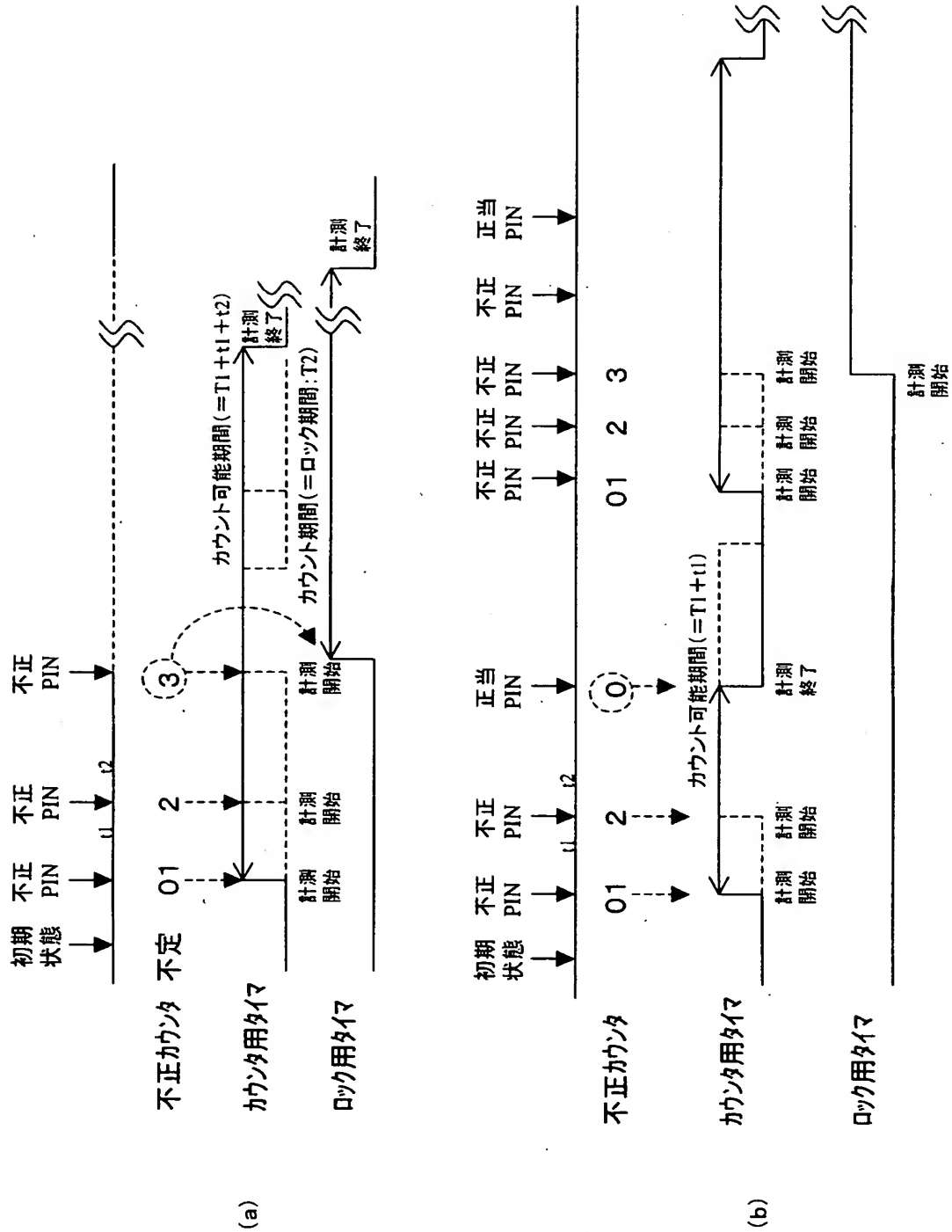
【図 12】



【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 端末装置や処理サーバなどのシステム側に負担をかけず、単体で一定時間の P I N ロックを実現できる I C カードの提供。

【解決手段】 利用時にのみ端末装置 1 0 から電力供給を受けて所定の処理を行う I C カード 1 0 は、利用時に端末装置 1 0 から入力される P I N を R O M 3 3 に備える固有の P I N で照合する。この照合の結果、不正 P I N である場合に、その入力回数を E E P R O M 3 5 で記憶する。この入力回数が予め定めた閾値となったとき、ロック用タイマ 3 6 で計測を開始し、この計測期間中には前記照合を行わない。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 7 3 5 6 5
受付番号	5 0 2 0 1 9 5 7 6 2 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 1 月 6 日

< 認定情報・付加情報 >

【提出日】 平成 14 年 12 月 25 日

次頁無

特願 2002-373565

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日
 [変更理由] 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝

2. 変更年月日 2003年 5月 9日
 [変更理由] 名称変更
 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝